Conducting Efficient Insider Threat Investigations using KAPE
Notes:

- Session is being recorded, You’ll receive access to the recording in a couple days

- Ask questions via chat >

- We’ll try to answer as many questions as possible
Upcoming KAPE Intensive Training and Certification

- Virtual live sessions
- Max 25 students

bit.ly/kape2020

<table>
<thead>
<tr>
<th>SCHEDULE</th>
<th>INSTRUCTORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 30, 2020</td>
<td>Eric Zimmerman</td>
</tr>
<tr>
<td>10:00 a.m. – 7:00 p.m. (EST)</td>
<td>Mari DeGrazia</td>
</tr>
<tr>
<td></td>
<td>Sean Straw</td>
</tr>
<tr>
<td></td>
<td>Scott Zuberbuehler</td>
</tr>
<tr>
<td>October 8, 2020</td>
<td>Paul Wells</td>
</tr>
<tr>
<td>8:00 am – 5:00 pm (BST)</td>
<td>James Thoburn</td>
</tr>
</tbody>
</table>
About Tony & Aaron

• Senior Vice Presidents at Kroll

• Former in-house experience leading insider threat investigations
Overview

- Insider Threat Investigations
- Collection Efficiency
- Analysis Efficiency
- KAPE Case Studies
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR? *  

- Leaks of internal information: 39%  
- Data theft: 29%  
- Reputational damage due to third-party relationships: 29%  
- Fraud by external parties: 28%  
- Fraud by internal parties: 27%  
- Disruption due to sanctions, tariffs, etc.: 27%  
- Adversarial social media activity: 27%  
- IP theft: 24%  
- Bribery and corruption: 23%  
- Counterfeiting or gray market activity: 17%  
- Money laundering: 16%  

* Kroll Global Fraud and Risk Report, 2019-20

KROLL IR CASES RELATED TO UNAUTHORIZED ACCESS

* Kroll internal data as of August 2020
Insider Threat Investigations | Why Does This Matter?

- What is insider threat – intentional/unintentional
- Based on management, policies, etc.
- Plethora of scenarios – this affects everyone, etc.
- Time is of the essence
- Exigent circumstances – departing employees (NDAs, non competes, etc.), leaving the country, etc.
- ROI = Time = more investigations
Collection Efficiency
Collection Efficiency | Overview

• KAPE targets key forensic artifacts required for analysis and runs in a matter of minutes
• Can be used for remote and/or automated collections
• Can be shared on a USB for single-click collections for non-technical users
• Can send to various destinations, including SFTP, S3, etc.
## Collection Efficiency | Basic Targets

<table>
<thead>
<tr>
<th>Category</th>
<th>Target File Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Logs</td>
<td>Windows Event Logs</td>
</tr>
<tr>
<td>Evidence of Execution</td>
<td>Prefetch</td>
</tr>
<tr>
<td></td>
<td>RecentFileCache</td>
</tr>
<tr>
<td></td>
<td>Amcache</td>
</tr>
<tr>
<td></td>
<td>Syscache</td>
</tr>
<tr>
<td>File System</td>
<td>$MFT</td>
</tr>
<tr>
<td></td>
<td>$LogFile</td>
</tr>
<tr>
<td></td>
<td>$UsnJrnl:$J</td>
</tr>
<tr>
<td></td>
<td>$Secure:$SDS</td>
</tr>
<tr>
<td></td>
<td>$Boot</td>
</tr>
<tr>
<td></td>
<td>$Tops:$T</td>
</tr>
<tr>
<td>LnkFilesAndJumpLists</td>
<td>User Jumplist directories</td>
</tr>
<tr>
<td></td>
<td>User Office Recent .LNK files</td>
</tr>
<tr>
<td></td>
<td>User Recent and Desktop .LNK files</td>
</tr>
<tr>
<td></td>
<td>Restore Point (XP) .LNK files</td>
</tr>
<tr>
<td>Category</td>
<td>Target File Contents</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PowerShellConsole</td>
<td>ConsoleHost_history.txt</td>
</tr>
<tr>
<td>RecycleBinMetadata</td>
<td>Contents (including deleted files) of User Recycle Bin folders</td>
</tr>
<tr>
<td>RegistryHives</td>
<td>User (including UsrClass.dat) and system Registry hives and transaction logs</td>
</tr>
<tr>
<td>ScheduledTasks</td>
<td>SchedLgU.txt and scheduled task files</td>
</tr>
<tr>
<td>SRUM</td>
<td>Contents of Windows\System32\sru folder</td>
</tr>
<tr>
<td>ThumbCache</td>
<td>User thumbcache_*.db files</td>
</tr>
<tr>
<td>USBDevicesLogs</td>
<td>Setupapi.log and Setupapi.dev.log</td>
</tr>
<tr>
<td>WindowsIndexSearch</td>
<td>Windows.edb</td>
</tr>
</tbody>
</table>
Collection Efficiency | Build a KAPE Package

**Default KAPE Files & Folders (~150 MB)**
- Documentation
- Modules
- Targets
- ChangeLog.txt
- Get-KAPEUpdate.ps1
- gkape.exe
- kape.exe

**Files & Folders Needed for Triage Collection (< 10mb)**
- Targets
- kape.cli
- kape.exe
Collection Efficiency | _kape.cli

--tsource C: --tdest .\%m --target !BasicCollection --vhdx %m

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--tsource</td>
<td>C:</td>
<td>Use C:\ as the collection source</td>
</tr>
<tr>
<td>--tdest</td>
<td>.%m</td>
<td>Write output to subfolder named by hostname in directory where KAPE is run</td>
</tr>
<tr>
<td>--target</td>
<td>!BasicCollection</td>
<td>Use the !BasicCollection set of Targets</td>
</tr>
<tr>
<td>--vhdx</td>
<td>%m</td>
<td>Write output into a VHDX file named by the hostname</td>
</tr>
</tbody>
</table>
Collection Efficiency | Running KAPE

KAPE version 0.9.3.0 Author: Eric Zimmerman (kape@kroll.com)

KAPE directory: E:\Kape
Command line: --tsource C: \-tdest .\LT-11234 --target !BasicCollection --vhdx LT-11234

Using Target operations
Creating target destination directory 'E:\Kape\LT-11234'
Found 12 targets. Expanding targets to file list...
Cannot find target file "\...
Found 1,309 files in 0.70s

Copied deferred file 'C:\users\aaron.j_read\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db' to 'E:\Kape\LT-11234\users\aaron.j_read\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db'. Hashing source file...

Copied deferred file 'C:\users\aaron.j_read\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db' to 'E:\Kape\LT-11234\users\aaron.j_read\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db'. Hashing source file...

Copied deferred file 'C:\users\aaron.j_read\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db' to 'E:\Kape\LT-11234\users\aaron.j_read\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db'. Hashing source file...

Copied deferred file 'C:\programdata\microsoft\searchdata\data\applications\windows\Windows.edb' to 'E:\Kape\LT-11234\programdata\microsoft\searchdata\data\applications\windows\Windows.edb'. Hashing source file...

tant.evtx' due to IOException...
shooter.evtx' due to IOException...

Copied 1,083 (Deduplicated: 245) out of 1,338 files in 193.0738 seconds. See '_CopyLog.csv' in the VHDX(X)/Zip located in...

E:\Kape\LT-11234\copylog.csv' for copy details
to IOException...

Initializing VHDX creation. This may take a while...
to IOException...

VHDX file 'E:\Kape\LT-11234\2020-09-23T185526_LT-11234.vhdx' created.
to IOException...

Cleaning up files in 'E:\Kape\LT-11234'...

Compressing VHDX file to 'E:\Kape\LT-11234\2020-09-23T185526_LT-11234.zip'...

Done. Original size: 2.4GB, Compressed size: 477.7MB

Total execution time: 274.7489 seconds
Collection Efficiency | Storage/Transfer Options

- Local drive (USB)
- Network share
- Transfer to SFTP, S3, Azure, etc.

![Storage/Transfer Options Diagram]
Analysis Efficiency
Analysis Efficiency

What are Modules?

• The actual “processing” of the artifacts you collected
• Grouped in Categories

Can be Tailored

• What works for someone may not work for you
• Special Programs/Scripts can be utilized
Creating a Module

• Benefits of KAPE:
  – Open Sourced
  – Well Documented
  – Modules written in YAML
  – Frequently Updated by Community
  – Internally Created do not need to be shared
  – Select the Result format for your needs
  – Automation and Speed
  – Small Storage Footprint

• Creating the Internal Toolkit:
  – Proprietary based Investigations
  – Create Case Specific Modules
    » Run certain processes for certain investigations
  – If its Command Line, you can run it
Case Studies

- Intellectual Property Theft
- Exceeding Authorized Authority
- Custom Targets
Case Study – Intellectual Property Theft

• A senior engineer recently left the company and created his own business with a competing product offering.
• You are requested to determine if evidence exists that the engineer took data leading up to their departure.
• Artifacts of Interest:
  – USB Devices
  – File/Folder Access
  – Program Execution
Case Study – Intellectual Property Theft – USB Devices

Module: Registry\RECmd

Module: Event Logs
## Case Study – Intellectual Property Theft – File/Folder Access

**Module: File-Folder Access\Shellbags**

<table>
<thead>
<tr>
<th>AbsolutePath</th>
<th>CreatedOn</th>
<th>ModifiedOn</th>
<th>FirstInteracted</th>
<th>LastInteracted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop\D:\</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop\D:\Project-912328</td>
<td>1/12/2018 15:31</td>
<td>12/20/2017 11:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop\D:\Project-547891</td>
<td>2/1/2018 11:14</td>
<td>12/16/2017 16:22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop\E:\</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Case Study – Intellectual Property Theft – Program Execution

**Module: Registry\UserAssist**

<table>
<thead>
<tr>
<th>BatchValueName</th>
<th>ProgramName</th>
<th>RunCounter</th>
<th>LastExecuted</th>
</tr>
</thead>
<tbody>
<tr>
<td>\1NP14R77-02R7-4R5Q-O744-2RO1NR519807\abgrcnq.rkr</td>
<td>{System32}\notepad.exe</td>
<td>7</td>
<td>03/27/2018 09:23:15</td>
</tr>
<tr>
<td>Zvpobfbsg.ZvpobfbsgRqtr_Bjrxl03q80o0rj!ZvpobfbsgRqtr</td>
<td>Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge</td>
<td>1</td>
<td>03/27/2018 09:28:51</td>
</tr>
<tr>
<td>P:\Hhref\wpybhql\Qbjaybnqf\vafgnyyonpxhcnaqflap.rkr</td>
<td>C:\Users\cloudy\Downloads\installbackupandsync.exe</td>
<td>1</td>
<td>03/27/2018 10:40:33</td>
</tr>
<tr>
<td>P:\Hhref\wpybhql\Qbjaybnqf\Renfre 6.2.0.2982.rkr</td>
<td>C:\Users\cloudy\Downloads\Eraser 6.2.0.2982.exe</td>
<td>1</td>
<td>03/27/2018 10:43:48</td>
</tr>
<tr>
<td>P:\Cebtenz Svyrf\Renfre\Renfre.rkr</td>
<td>C:\Program Files\Eraser\Eraser.exe</td>
<td>1</td>
<td>03/27/2018 10:51:12</td>
</tr>
<tr>
<td>P:\Hhref\Choyvp\Qrfxgbc\Renfre.yax</td>
<td>C:\Users\Public\Desktop\Eraser.Ink</td>
<td>1</td>
<td>03/27/2018 10:51:12</td>
</tr>
</tbody>
</table>
Case Study – Exceeding Authorized Access

• Alert received for IT employee emailing sensitive data outside of the company.
• You are requested to determine what the materials are and where they came from.
• Artifacts of Interest:
  – LNK Files
  – $MFT
Case Study – Exceeding Authorized Access – File/Folder Access

Module: FileFolderAccess\LECmd

<table>
<thead>
<tr>
<th>SourceFile</th>
<th>SourceCreated</th>
<th>SourceModified</th>
<th>WorkingDirectory</th>
<th>MachineID</th>
</tr>
</thead>
<tbody>
<tr>
<td>D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\Profile Pic.jpg</td>
<td>6/6/2020 11:45</td>
<td>6/6/2020 11:45</td>
<td>\dt-cperry\c$\users\cjerry\Desktop\Profile Pic.jpg</td>
<td>dt-cperry</td>
</tr>
<tr>
<td>D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\Perry Taxes.pdf</td>
<td>6/6/2020 11:47</td>
<td>6/6/2020 11:47</td>
<td>\dt-cperry\c$\users\cjerry\Documents\Taxes\2019\Perry Taxes.pdf</td>
<td>dt-cperry</td>
</tr>
<tr>
<td>D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\EmployeeDetails20200101.xlsx</td>
<td>6/6/2020 11:51</td>
<td>6/6/2020 11:51</td>
<td>\dt-cperry\c$\users\cjerry\Documents\Projects\HR\EmployeeDetails20200101.xlsx</td>
<td>dt-cperry</td>
</tr>
<tr>
<td>D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\All.Employee.Listing.2020-03-01.csv</td>
<td>6/6/2020 9:37</td>
<td>6/6/2020 9:37</td>
<td>\dt-ljones\c$\users\ljones\Documents\All.Employee.Listing.2020-03-01.csv</td>
<td>dt-ljones</td>
</tr>
<tr>
<td>D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\img6001.jpg</td>
<td>6/6/2020 12:49</td>
<td>6/6/2020 12:49</td>
<td>\lt-sjohson\c$\users\sjohnson\OneDrive\Documents\Pics\img6001.jpg</td>
<td>lt-sjohson</td>
</tr>
<tr>
<td>D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\img5123.jpg</td>
<td>6/6/2020 12:53</td>
<td>6/6/2020 12:53</td>
<td>\lt-sjohson\c$\users\sjohnson\OneDrive\Documents\Pics\img5123.jpg</td>
<td>lt-sjohson</td>
</tr>
<tr>
<td>D:\users\djones\AppData\Roaming\Microsoft\Windows\Recent\img5124.jpg</td>
<td>6/6/2020 12:54</td>
<td>6/6/2020 12:54</td>
<td>\lt-sjohson\c$\users\sjohnson\OneDrive\Documents\Pics\img5124.jpg</td>
<td>lt-sjohson</td>
</tr>
</tbody>
</table>
Case Study – Exceeding Authorized Access – File/Folder Access

Module: FileSystem\MFTECmd_$MFT
Case Study – Custom Target/Modules

- Corporate Proprietary Investigation
  - Not an IR Event
- Geographically separated
  - No Travel permitted
- User may have stored IP in folders throughout the OS Structure
  - Files had a unique file extension
- Needed to be as forensically sound as possible
  - Kape created .zip file + password protection
Case Study – Custom Target/Modules – What We Did

• Created a unique Target that would look for specific file extension
• Created a unique Module for fast processing of specific artifacts
• Remoted into the machine when the user had the machine on network
• Initiated KAPE Target to pull the artifacts
• Ran KAPE Module to process the artifacts needed, which included a nice file listing
• On the machine for less than 10 minutes
• Processing of the Targeted artifacts took even less than that
• Customer was provided preliminary reports within 8 hours of our involvement
Case Study – Custom Target/Modules – Quick Wins

• Insider Threat allegation was substantiated very quickly
• Amount of dwell time was minimal
  – customer was not even prepared for returned results
• No Expenses
  – Saved thousands of dollars alone on no expenses needed
• Internally proved the tool could be leveraged for more than just IR
  – Tailoring to specific files relevant to the matter
• Tailoring the tool saved countless hours on the target system
  – User never knew we were there
Questions
For More **KAPE:**
Intensive Training and Certification

- Virtual live sessions
- Max 25 students

**bit.ly/kape2020**

<table>
<thead>
<tr>
<th>SCHEDULE</th>
<th>INSTRUCTORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 30, 2020 10:00 a.m. – 7:00 p.m. (EST)</td>
<td>Eric Zimmerman</td>
</tr>
<tr>
<td></td>
<td>Mari DeGrazia</td>
</tr>
<tr>
<td></td>
<td>Sean Straw</td>
</tr>
<tr>
<td></td>
<td>Scott Zuberbuehler</td>
</tr>
<tr>
<td>October 8, 2020 8:00 am – 5:00 pm (BST)</td>
<td>Paul Wells</td>
</tr>
<tr>
<td></td>
<td>James Thoburn</td>
</tr>
</tbody>
</table>
For more information about our global locations and services, please visit:

www.kroll.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.